Wells Fargo & Company
Law Department
633 Folsom Street, 7th Floor
San Francisco, CA 94107

14

Via Electronic Mail

October 14, 2003

Public Information Room
Office of the Comptroller of the Currency
2520 E Street, S.W.
Mail Stop I-5
Washington,D.C. 20219
Attention: Docket No. 03-18

Mr. Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, D.C. 20429
Attention: Comments/OES

Ms. Jennifer J. Johnson
Secretary, Board of Governors
Of the Federal Reserve System
20th Street and Constitution Ave. N.W.
Washington, D.C. 20551
Attention: Docket No. OP-1155

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552
Attention: No. 2003-35

Re: Proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Ladies and Gentlemen:

Wells Fargo & Company ("Wells Fargo") appreciates the opportunity to comment on the proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Wells Fargo is a diversified financial services company which includes more than 25 national banks, a mortgage company, a consumer finance company, securities brokerage, investment advisors and insurance agencies.

1. General

We generally support the proposition that such a response program is an important part of a financial institution's information security program, and that customer notification should be given when it is likely to serve some useful purpose. Indeed, Wells Fargo has had an incident response component in its information security policy for many years. We have also notified affected customers of information security breaches when it appeared that such notification might prevent or mitigate misuse of

customer information, even in the absence of any express legal obligation to provide such notice.

However, we are concerned that the proposed "guidance" may be interpreted as mandating an inflexible list of steps which must be taken and items which **must be included** in each customer notification, rather than factors which **should be considered** while reserving flexibility to respond appropriately to the unique circumstances of teach incident.

Flexibility is especially important in view of the existing California law (SB 1386 (2002), Civil Code Section 1798.84) and the proposed federal bill S.1350) requiring notice to customers (and others) in the event of information security breaches. Institutions covered by the proposed Guidance should not be forced to walk a tightrope between inconsistent sets of requirements.

Some specific areas in which we believe the proposed Guidance could be improved are as follows:

2. "Sensitive Information"

Since the obligation to notify affected customers is triggered primarily by whether "sensitive information" has been compromised, the definition of this term is crucial to the obligations of covered institutions. We believe that the overriding consideration should be whether the compromise of a particular information element or combination of information elements significantly increases the risk that a consumer will become a victim of identity theft or other fraud. For example:

(a) Encrypted data should normally not be considered "sensitive" (this principle is reflected in CA SB 1386 and S.1350) unless there is reason to believe the encryption has been or is likely to be broken.

(b) "Account number" should not always be presumed to be sensitive. For example, checking account numbers are widely available because of the circulation of checks as part of the normal payments process. "Theft" of a checking account number alone may not represent a material increase in risk to the account owner. Still, the number of an installment credit account may be of virtually no use to a would-be fraudster. Still other types of account numbers may be of little or no value without a PIN, password or other access code or device. Again, CA SB 1386 and S. 1350 recognize that compromise of just an account number may not be enough to trigger customer notice requirements.

3. Customer Notification

Similarly, customer notification should be required only if – and when – such notice will provide a meaningful opportunity to help prevent or reduce harm to either the customer or the institution in a cost-effective manner. This general principle translates into several specific recommendations:

(a) There should be an explicit statement that, even if it is clear that customer notification will be required in a given case, it may be delayed (i) to complete remediation of any known vulnerability, or (ii) to avoid compromising any law enforcement or regulatory investigation. These temporary exceptions are found in S.1350 and CA SB 1386.

(b) The method of giving notice should be flexible enough to permit a balancing of the cost of notice against the likely benefits. For example, electronic (e-mail) notice should be permitted as to those customers for whom the institution reasonably believes it has reliable e-mail addresses. Also, "substitute" notice should be permitted when the number of affected customers is large or when it is impossible to determine which customers out of a large group were actually affected. Such substitute notice might consist of posting on the institution's web site and placement of advertisements or stories in widely-distributed news media. Again, this is consistent with S.1350 and CA SB 1386.

(c) When the breach occurs at a service provider, and there is reason to believe a substantial number of individually may be customers or more than one of the affected institutions, the service provider should be permitted to issue a joint notice on behalf of the affected institutions, so individual customers do not receive multiple notices relating to a single incident.

(d) The proposed Guidance should be amended to make it clear that the various items suggested for inclusion in any customer notice are, in fact, suggestions and not every item is mandatory in every customer notice. Just as each information security incident is unique, the notice (if any) needs to crafted to address those unique circumstances. Elements that may be appropriate in one notice may not be necessary or appropriate in the next.

4. Other Responses

In addition to the customer notice, there are other areas of a response program where more flexibility is needed than is currently provided in the proposed Guidance. In particular:

(a) Notification to the institution's primary regulator should only be required where there is a significant risk of harm to a significant number of the institution's customers. Some information security incidents may affect only a very small number of customers and may not be indicative of any systematic shortcoming; e.g., the improper disposal of a small number of paper records by a new employee. Such isolated incidents should not have to be reported to the institution's primary regulator.

(b) Flagging and securing accounts should only be required when there is reason to believe doing so will be a cost-effective way of reducing fraud losses for the institution and its customers. In some cases the nature of the information compromised (e.g., name, address and SSN) may make it unlikely that the customer's existing accounts will be the target of any fraud. In addition, it must be recognized that "securing" an existing account may cause the customer significant inconvenience, even if the institution absorbs all out-of-pocket costs (which may also be significant).

Conclusion

While we support the goals of the proposed Guidance, Wells Fargo believes it should indeed to "guidance," that is, a description of responses **to be considered**, rather than a mandatory list of things to be done. Because this will represent a major shift in the tone of the Guidance, we believe another draft should be proposed and published for comment. Since we believe most large financial institutions already follow practices which are largely similar to those proposed in the Guidance, we do not believe the addition of a few months to the approval process will seriously harm consumers.

If you have any questions regarding the foregoing, please contact me at (415) 396-0940 or mccorkpl@wellsfargo.com.

Sincerely yours,

Peter L. McCorkell